我国科学数据共享中的隐私治理探析*

■ 朱贝[1] 王传清[2]

[1] 广州医科大学图书馆 广州 511436 [2] 中国科学院文献情报中心 北京 100190

摘 要：[目的/意义]针对我国当前科学数据共享中的隐私问题，探索隐私治理方法和对策以便更好地实现科学数据共享。[方法/过程]运用文献调查法和建模法，在厘清科学数据共享隐私问题的基础上，提出4项隐私治理原则，构建隐私治理模型，探索科学数据共享中的隐私治理对策。[结果/结论]可以采用完善隐私保护法律体系、加强隐私保护配套制度建设、采用隐私增强技术、提升利益相关者隐私素养、构建隐私伦理保护规制、加强科学数据流程管理等措施来实施隐私治理，从而有效促进科学数据共享。

关键词：科学数据共享 隐私治理 治理对策

分类号：G203

DOI：10.13266/j.issn.0252－3116.2020.22.004

如今，数据成为像石油一样重要的战略资源，是企业和政府机构提升创新力与竞争力的关键要素之一。企业和政府机构收集了大量的数据，这些数据通常使用统计和数据挖掘方法进行分析。当这些方法在收集数据的企业内部使用时，敏感信息的泄露风险是有限的。但当数据由第三方进行分析时，敏感的隐私信息保护就变成了一个紧要问题。国外调查发现，数据泄漏是头号威胁，排名高于病毒、木马和蠕虫病毒[1]。数据和信息系统正面临越来越多各种来源的隐私威胁，如人们的好奇心、员工行为、计算机辅助欺诈、网络攻击、网络钓鱼、蓄意破坏、盗窃、火灾或基础设施事故[2]。妥善治理科学数据共享中的隐私问题，是确保科学数据安全、加快推动科学数据在各学科领域深度融合与应用发展的重要保障。目前鲜有学者深入探讨我国科学数据共享中的隐私治理问题。本文通过文献调查，在厘清科学数据共享中的隐私问题基础上，构建隐私治理原则和模型，从法律、制度、技术、隐私素养、伦理、数据流程管理等6个维度全面探讨科学数据共享中的隐私治理对策，以期实现我国科学数据共享和隐私保护的平衡与发展，更好地促进科学数据共享。

1 国内外相关研究述评

虽然鲜见专论科学数据共享中的隐私治理的成果，但不能忽视国内外已就该主题的相关问题，如科学数据共享中的隐私或数据隐私、信息隐私、隐私法律与政策、隐私保护技术、隐私保护措施、隐私伦理、隐私治理等内容作了广泛探索。

大多数观点认为，隐私是指“与公共利益、群体利益无关，当事人不愿让他人知道或是他人不便知道的信息，当事人不愿他人干涉或他人不便干涉的个人私事，以及当事人不愿他人侵入或他人不便侵入的个人领域”[3]。基于此观点，可以认为，科学数据共享中的隐私是指在遵循相关共享协议基础上，运用多种共享手段和方式，公开发布科学数据这一行为过程中的个人、组织或机构不愿或不便为他人所知道和干涉的私人信息、私人事务与私人领域。科学数据共享中的隐私与数据隐私是不同的概念。数据隐私是数据管理的一个分支，是指设立不同程度的管制来保护数据不受第三方侵犯，必要时取得数据主体的同意，并维持数据的完整性[4]；它也是信息技术的一部分，帮助个人或组织确定系统中的哪些数据可以与他人共享，哪些数据应该受到限制[5]。因此，科学数据共享中的隐私与数据隐私并非同一个概念，两者既有交叉又有不同。此外，科学数据共享中的隐私也不等同于信息隐私。信息隐私不仅包含数据隐私，还包含人际交往隐私[6]，且信息隐私范畴不仅限于个人，网络环境中的群体信息

* 本文系国家社会科学基金项目“开放科学环境下的科学数据开放共享机制与对策研究”（项目编号：18ATQ007）研究成果之一。

作者简介：朱贝（0000－0002－0688－6055），助理馆员，硕士；王传清（ORCID：0000－0002－2686－8153），编辑，博士，通讯作者，E-mail：wangcq@mail.las.ac.cn。

收稿日期：2020－06－09 修回日期：2020－07－29 本文起止页码：37－47 本文责任编辑：易飞

隐私需依据隐私情境进行更深入细致的划分[7]。科学数据共享中的隐私包含共享过程中的个人隐私、行为隐私、人际交往隐私和数据隐私，比信息隐私的研究维度更宽泛，且隐私主体也不仅限于个人，是共享过程中的利益相关者。科学数据共享中的隐私利益相关者可以是作为组织者的科研机构、作为使用者的用户、作为传播者的出版商或数据库商等。

在隐私法律与政策方面，2018年5月欧盟通过并实施的《一般数据保护条例》是一项内容丰富的综合性数据保护法律，可让科学研究的监管更灵活和有章可循，促进科学数据的再利用与跨国共享[8]。该条例提供了一系列更具操作性的隐私保护要求与规范，扩大了隐私保护的适用范围，提高了隐私侵权惩罚力度，为世界其他国家制定科学数据共享中的隐私法律提供了范例[9-10]。此外，在科学数据共享过程中必须遵循相关国家或地区的法律政策惯例以保护个人隐私[11]，且个人隐私保护政策与科学数据开放政策存在共通点，都应注重实现个人利益与公共利益的平衡[12]。国内学者调研了英澳等国科学数据共享过程中的个人隐私保护政策，建议从明确隐私保护范围、遵守数据保护政策及道德规范、采用问责机制等方面借鉴制定符合我国国情的科学数据隐私保护政策[13]。

在隐私保护技术方面，主要包括差分隐私技术和数据加密技术等。差分隐私技术是一种通过注入噪声使数据失真，从而保护数据集中个体隐私的技术方法[14]。利用基于差分隐私技术且具有高实用价值的轨迹数据发布系统——DP-Star系统，可以对交通导航数据涉及的移动用户的隐私进行安全保护[15]。数据加密技术是通过对敏感数据进行密文处理输出，接收后进行解密还原为明文的一种加密方法[16]。可通过密文检索确保用户查询隐私和数据隐私安全，通过属性加密可动态撤销用户的访问权限[17]。此外，还可使用无人工操作的“可信服务器”(Trusted Server)确保医学、教育和经济等领域科学数据集中包含的个人敏感信息不被数据管理者读取、操纵或泄露[18]。整合多来源的数据关联分析技术是当前隐私保护面临的重大挑战，应重点做好前端的隐私保护，并在共享过程中采用加密技术加大对重要数据的保护力度[19]。

在隐私保护措施方面，有人认为应该坚持“可寻找、可访问、可互操作、可重复利用”原则对有关热带环境气候的科学数据进行采集与管理，确保数据隐私安全[20]；也可采用审核批准、病人数据识别、个人同意等预防手段来确保卫生信息研究中的隐私安全[21]；或者采取加强对网络和数据服务器的审查、优化数据存储程序等措施来确保医疗研究中敏感数据的隐私安全，并提高科学数据共享的效用[22]。

此外，科学数据共享中的隐私面临敏感数据难以保护、隐私数据被贩卖给商家、通过大数据画像可确定隐私主体身份等伦理困境[23]。面对科学数据共享中的隐私伦理失范现象，可通过树立正确的伦理价值观、加强伦理监管等方式来避免隐私泄露[24]。

不过，目前人们对隐私治理定义没有形成共识。隐私治理指导方针包括数据收集限制原则、数据质量原则、目的明确化原则、利用限制原则、安全保护原则、开放原则、个人参与原则、问责原则等隐私治理原则[25]。网络空间的隐私治理应包括政府、企业、组织或机构中的个人这三个主要行动者采取一定的法律政策或实际行动以实现数据保护[26]。可以认为，科学数据共享中的隐私治理是以科学数据共享中的隐私保护、隐私泄露、隐私侵权等隐私问题为治理对象，在遵循一定的隐私治理原则基础上，通过综合采用政策法规、管理制度、技术与伦理规范等治理措施和行动，实现科学数据共享价值最大化和隐私风险最小化的治理目标。其治理内容既包括对科学数据的治理，也包括对隐私相关利益主体及共享过程、共享环境的治理。

2 科学数据共享中的隐私问题分析

由于科学数据共享是收集、组织、发布、传播和利用科学数据的过程[27]，因此，科学数据共享中的隐私问题存在于数据收集、数据组织、数据发布、数据传播、数据利用5个阶段，主要涉及隐私保护、隐私泄露、隐私侵权问题，具体表现如下7种情形：

2.1 隐私保护法律体系不完善

我国大陆地区目前已颁布、直接提及“隐私”的相关法律有《网络安全法》《侵权责任法》《民事诉讼法》《刑事诉讼法》《未成年人保护法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》[28]，以及2020年5月最新通过的《民法典》[29]等。另颁布有《科学数据管理办法》行政管理政策，对科学数据的共享利用、保密与安全等作了相关规定[30]，但暂无法律条款直接对科学数据共享中的隐私予以保护。因此，我国科学数据共享中的隐私法律保护力度仍比较薄弱，主要表现是：①无论是公法还是私法，我国都未将隐私权作为一种独立的权利加以规定和保护。现有法律尚未对隐私范围作明确划分，且我国对隐私保护的法律分布于多部法律条款中，立法过于分散笼统，缺乏

综合性、系统性、专门性的隐私法律保护。②我国已有的隐私保护法律互通性差，而且条款内容明显滞后社会发展，针对性和实际操作性不强[31]。尤其是为应对大数据新形势的变化发展，多国都已颁布了数据隐私治理的相关法律文件，而我国在这一领域的法律政策保护还比较落后，且法律保护层级较低，过于笼统窠臼，互通性差，不能从根本上解决隐私保护法律体系薄弱的问题[32]，如现已实施的《信息安全技术个人信息安全规范》国家标准，规定"个人信息经匿名化处理后所得的信息不属于个人信息"，但随着生物医学技术的发展，个人健康隐私信息内容有所变迁，可根据基因组数据预测个人面部结构、身高、年龄、性别等个人隐私信息，因此该条款内容不适用于个人健康隐私信息[33]。我国亟需出台专门针对科学数据隐私治理的相关法律条款或政策规定，以更好地促进科学数据共享与利用。③缺乏隐私权救济机制[34]。在我国现有的隐私保护法律体系下，侵犯公众隐私权并造成重大影响时，法律对被侵权人的损害赔偿无详细指引，且隐私侵权行为发生时，用户与数据共享平台或企业在技术、资源等方面存在巨大差距，难以合理有效收集隐私侵权证据，仅仅依靠现有法律难以维护自身合法权益。2017年趣店疑超百万条学生信息被泄露，在黑市叫卖，所涉及信息包括学生电话、住址、学校、个人信贷信息等隐私，但因受害学生涉及范围广，侵权证据难收集，该企业仅在后续回应中称会加强数据安全能力和信息加密强度[35]。④跨境科学数据流动频繁，但跨地区的隐私保护法律条款具有一定差异性，缺乏统一规范标准，且各国在制定数据保护条例时设置有跨境数据保护壁垒，会最大限度保护本国居民权益，与国际保护法律适用的原则相背，保护难度加大[36]。

2.2 隐私保护配套制度不合理

科学数据共享中的隐私保护配套制度不合理，主要表现在以下几方面：①科学数据共享中的隐私限制制度不完善。在科学数据组织过程中，数据搜集者和使用者会利用手中的技术优势对数据生产者的隐私数据进行过度收集和利用，造成隐私的过度披露[37]。工信部发布的《关于侵害用户权益行为的APP通报(2020年第二批)》文件显示，多款教育类APP存在过度收集个人信息并私自共享给第三方等严重侵害用户权益的问题[38]，这些软件可读取用户的电话号码、短信、通讯录等用户隐私，过度索取权限，危害未成年人隐私信息安全。在科学数据共享利用阶段，涉及隐私的共享协议或规范标准是由数据搜集者或使用方制定的，隐私保护的力度与范围对隐私主体来说缺乏可控性与自由性，且大多数科学数据共享平台的隐私政策内容相似且空泛，权限不明确，实际操作性低。"净网2020"专项行动中，有部门监测到医疗和在线教育类等移动应用存在未向用户明示申请的全部隐私权限、未说明收集使用个人信息规则等涉嫌隐私不合规的行为[39]。②缺乏第三方问责制度。在整个科学数据共享生命周期中，缺乏独立于用户和服务方的第三方监督机构开展数据监管和隐私保护工作，实施隐私审查监控制度、公开曝光制度、奖惩制度等[40]。③缺乏行业自律制度体系。美国采取的是行业自律为主、法律限定为辅、政府不过度干预的隐私保护制度体系，但我国在法律体系不完善的现状下，行业自律也未充分发挥应有的约束作用去推动隐私保护[41]。

2.3 隐私保护技术性能不足

隐私保护技术性能的高低可从数据的准确性、隐私性、延时性等方面进行评估[42]。目前科学数据共享中使用较多的是基于数据加密技术和匿名技术的隐私保护方法，其性能都存在一定不足。使用数据加密技术，隐私保护力度取决于密钥的复杂程度以及传输过程中密钥是否发生泄露，存在一定的风险。如著名的"CSDN密码外泄事件"，CSDN是一个中文IT技术交流平台，曾遭黑客攻击其密码库导致600多万用户的登录名、密码、邮箱等隐私信息被泄露[43]，给用户隐私保护造成严重威胁。匿名技术在隐私保护上也有一定的局限性。应用隐私保护技术的过程中通常会将隐私用匿名来表示，但实际上两者是存在一定区别的。因在隐私条件下，我们知道一个人的身份，但不知道相关的个人事实，而在匿名条件下，我们知道个人事实，但不知道相关人的身份。例如，匿名是对个人身份信息如姓名、性别、年龄等隐私数据进行匿名化处理，但对银行账户、信贷信息等敏感数据不作处理，而隐私则会对个人的银行账户、信贷信息等敏感数据进行保护。在匿名操作时，即使不知道一个人的具体个人收入，也可以知道他属于高收入群体，而知道这种信息本身就属于隐私的一种泄露和价值的损失。而且现有的匿名技术模型大部分基于删除个人标识属性，然后将准标识匿名化处理[44]。但因包含个人标识符的数据和完全匿名的数据之间经常未能明确区分，如果出于隐私考虑对所有类型的科学数据都施以限制性政策，虽能确保科学数据的时效性，却会损害科学数据的完整性[45]。此外，因为科学数据共享过程中的数据不是静态的，而是一直处在动态变化过程中，且数据体量会随

时间增长越来越大,如何在确保隐私的同时也确保数据价值的动态实现,当前隐私保护技术还难以解决。因此,现有科学数据共享过程中的隐私保护技术仍存在一定局限性,需进一步改进、提升其性能。

2.4 隐私保护意识缺乏

首先,信息时代下公民缺乏隐私保护意识主要表现是为对隐私数据的价值不够重视:在数据驱动经济中,数据身份商品化是新兴现实,个人数据具有一定的货币价值,虽然我国已经建有大数据交易平台,但目前我国个人数据资产权默认归为数据的收集者,由数据收集者开展数据交易,如 APP 企业通过收集用户个人隐私数据并贩卖给第三方,而个人数据的生产者则缺乏数据交易参与性[46];因此在科学数据共享中,隐私数据容易被视为一种"附带数据"而忽略其经济价值遭泄露。其次,隐私主体的保护意识缺乏:快捷有效的大数据挖掘技术可以让个人、组织或机构在共享过程中抓取大量的个人隐私数据,但事实上公民对网络平台的传播性质缺乏正确的认知,无法清楚区分个人与公共的隐私边界,缺乏隐私保护自觉,主动泄露隐私信息将导致个人隐私数据遭企业"二次利用"[47]。而且因互联网的共享性、虚拟性等特征,用户在科学数据的共享过程中,对隐私保护不够重视,容易因操作不当引发隐私泄露。近年来,政府及事业单位因工作人员隐私保护意识不强而过度披露相关人员隐私信息的新闻事件时有发生[48],给相关部门和个人造成了不良影响。此外,2019 年人民智库采集了全国各地近 4 000 份调查样本,结果显示,仅有 28.89% 的调查者会"主动采取措施保护个人隐私",且未采取过保护措施的调查者认为"隐私维权程序复杂""成本高"等妨碍了隐私维权[49],说明我国公民隐私主动维权的意识有待提高。再者,行业隐私保护自律意识缺乏。行业自律是指基于行业自行制定的规章制度或准则规范对行业进行自我管理或约束的一种制度[50]。目前,我国在推进科学数据共享过程中,较少有行业协会会采用相关隐私保护政策或规范、网络隐私认证或隐私选择平台等形式对行业行为进行约束,说明我国行业隐私自律保护普及率较低。

2.5 隐私泄露问题突出

近年来,科学数据共享中的隐私泄露问题越来越突出,给企业、个人造成严重损失和影响[51]:IBM 中国调研发现来自网络的恶意攻击是致使数据泄露的根本原因,且在过去 6 年的调研期间,因黑客攻击或犯罪攻击而引发的数据泄露事件的百分比已从 42% 上升至 51%(同比增长 21%),恶意数据泄露给调研中的受访企业带来平均 445 万美元的损失;且大规模数据泄露中一般都包含隐私信息和敏感数据,给用户隐私安全带来潜在威胁,如今年 4 月青岛胶州中心医院 6 000 余人就诊名单被泄露,并被谣传感染了新冠肺炎。造成隐私泄露问题突出的原因笔者认为主要包括:①科学数据共享中的隐私泄露一般体量庞大,涉及广泛,加大了隐私治理难度。2019 年国内一家主营面部识别、人工智能和安防业务的公司深圳视界(Sense Net)被曝泄露人脸识别数据,此次数据泄露事件涉及 256 万人共计 680 万条记录,包括个人身份证信息、人脸识别图像等隐私数据,任何人都可获取这些记录并跟踪个人行动轨迹[35]。②隐私悖论加剧了科学数据共享中的隐私泄露风险。即隐私主体明知隐私风险,但只要有一定回报,就会选择披露隐私或者忽略隐私泄露带来的威胁[52],造成科学数据共享中的隐私泄露恶性循环,这也是隐私泄露事件屡屡发生的原因之一。

2.6 隐私侵权现象严重

隐私侵权是指未经隐私主体"知情同意",通过某种方式或手段获取隐私的行为[53]。由于数据挖掘技术的广泛应用,导致越来越多的科学数据共享中的隐私泄露并引发隐私侵权现象,具体表现为窥探与监控、未经许可的商业利用、数据歧视、侵犯人身和财产安全、诈骗等侵权结果。如近期出现的"中信银行未经授权泄露客户隐私信息"被启动立案调查程序事件[54],是一起典型的未经许可商业利用的金融数据隐私侵权事件,引发社会较大反响。目前,科学数据共享中的隐私侵权现象严重的原因笔者认为主要有:①网络技术和数据挖掘导致监控无所不在,而数据又具有记忆性和组合型特征,即使删除隐私标签数据,也不能防止被再次窥探和利用[55];②大多数科学数据共享平台和网站的隐私保护政策设置为默认同意收集隐私信息,包括收集个人身份、消费记录、联系信息、习惯偏好等,并利用所收集到的隐私信息帮助第三方投放广告[56];③算法歧视导致在收集、产生和解释数据时产生与人类相同的偏见和歧视,如种族歧视、性别歧视、弱势群体歧视等与隐私有关的歧视[57]等。

2.7 隐私伦理的挑战

科学数据共享的实践中还面临隐私伦理问题带来的挑战。以医学科学数据为例,随着基因测序技术越来越普遍应用于生物医学研究领域,人类基因数据共享成为医学发展必然趋势,而基因组原始数据具有敏感性、唯一性等特征,应归属于个人隐私范畴的重要内

朱贝，王传清. 我国科学数据共享中的隐私治理探析[J]. 图书情报工作,2020,64(22):37 -47.

容,这就面临一个问题:其研究的参与者和患者是否有法律和道德上的权利来接收他们的基因组原始数据[58];其次,基因测序产生的数据在共享过程中具有一定的安全隐患,隐私保护和知情同意履行困难,且目前我国的伦理管理与伦理审核体系无法管理和指导医学数据共享中的伦理实践[59]。除医学健康数据面临挑战外,当前随处可见的"地毯式监控"对个人隐私造成威胁[60],也是隐私伦理重灾区,这些隐私伦理失范现象都会给科学数据共享发展带来挑战。

3 科学数据共享中的隐私治理原则与模型构建

因存在上述多种问题,笔者提出在遵循一定的隐私治理原则基础上,构建治理模型,以加强我国科学数据共享中的隐私治理。

3.1 隐私治理原则

为推动科学数据共享中的隐私保护,隐私治理原则首先应坚持合理、合法、平等、公平性原则,笔者认为隐私治理原则可从以下几点关注:

3.1.1 明确数据权属,平衡公私权利

在大数据产业迅猛发展的背景下,科学数据的保护与利用矛盾日益凸显,数据权不仅包含财产权,也包含隐私权。因数据是一种非物质性新型资源,明确数据权利到底是归属于个人、网络平台、公众或是个人与平台共有,可依据具体场景界定,有利于数据的隐私保护基于"场景性公正"[61]。公权利指以维护公众利益为目的的权利,私权利指以满足个人需要的为目的的私人权利[62]。目前不论是国外还是国内隐私法律保护框架体系,主要施行以"用户为中心的单边保护"框架,更多关注隐私保护的个体意义,但存在隐私保护难履行或效率低下等弊端[63]。因此在其治理过程中,应注重保障隐私主体权益,明确公、私权主体的权利义务,切实保护私权主体的知情权、平等对待权,在隐私权的保护与公众利益之间寻找平衡点,通过法律条文或国家政策加以调控,促进二者关系平衡协调。

3.1.2 坚持收集限制和目的明确原则

在科学数据共享过程中,坚持收集限制原则是指收集过程中应采取合法且公正的手段,根据需求收集相关数据,尽量避免因全方位、大数量、高强度采集数据使隐私主体利益遭受损害;坚持目的明确原则是在共享过程中除非隐私主体同意或法律允许,科学数据所涉及的隐私部分不得用于明确化目的以外的目的使用。即在告知隐私主体科学数据共享是用于合法的特定目的后,不能随意更改、限制科学数据的利用,否则需取得隐私主体的重新同意。如在新冠肺炎疫情防控期间,采用大数据技术进行疫情数据采集和分析可以更高效精准,但也出现了个人信息泄露现象,因此应提升疫情防控中个人信息防护标准,明确禁止将疫情防控中搜集的个人数据进行商业利用,严格加以保护[64]。

3.1.3 坚持公开性和安全保护原则

公开性原则的前提坚持科学数据开放为常态,不开放为例外[30],以促进科学数据的共享发展。即当隐私主体利益与国家安全利益发生冲突时,以国家安全为优先。且公开性原则要求公开科学数据共享运行环节、相关政策及规章制度,实现对科学数据共享的隐私保护公共监督,有利于维护隐私主体的知情权。安全保护原则是指科学数据共享中的所有参与者应积极采取安全可靠的有效保障措施,包括软硬件措施,确保数据发布的准确性、完整性、可用性,避免数据在共享过程中遭受损害或泄露。

3.1.4 坚持多主体参与,协同治理原则

在公共事务治理过程中,以市场为主导或以政府为主导的单一中心治理方式存在"公地悲剧"、"囚徒困境"、公共政策错误或执行率低等困境,建立"市场""政府"和"社会"框架下的"多中心"治理模式有利于发挥社会自主组织与公众积极性,促进公共事务可持续发展[65]。因此在科学数据共享中的隐私治理中,坚持构建以政府部门、企业、研究机构、出版商、行业协会、研究人员、用户等多元主体参与、协同治理的模式和格局有利于平衡隐私保护的主动权和控制权,促进隐私保护由粗放型向精细化转变。

3.2 隐私治理模型的构建

基于国内外已有的研究成果,在遵循上述治理原则基础上,以科学数据共享中的隐私问题为导向,采用包括政策法规、管理制度、技术、隐私素养、伦理规范、数据流程管控等在内的多种治理措施,可以构建科学数据共享中的隐私治理模型(见图 1)。

该模型以隐私治理为核心,针对科学数据共享中的隐私保护、隐私侵权、隐私泄露等问题,从法律、制度、技术、隐私素养、伦理、数据流程管理等 6 个维度,采用相关治理对策来破解隐私治理困境。

该模型的构建遵循以上隐私治理原则,对科学数据共享中的隐私治理具有良好的指导和规范作用。从治理对象来看,宏观层面而言,因科学数据共享中的隐

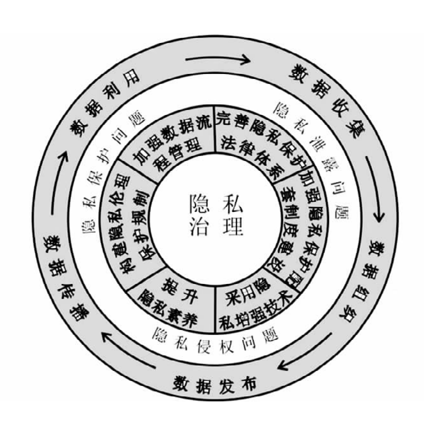


图 1　科学数据共享中的隐私治理模型

私治理始终贯穿于科学数据生命周期的收集、组织、发布、传播、利用 5 个阶段，其治理对象应是存在于科学数据行业、环境、共享过程中涉及的隐私保护、隐私侵权、隐私泄露等隐私问题。微观层面而言，是对科学数据共享过程中产生或需要的隐私信息、隐私事务、隐私领域的治理。因此，该模型选取的治理对策有从法律、配套制度、伦理环境等宏观层面的部署，也有从技术、隐私素养、数据流程等微观层面的开展。从治理主体来看，参与隐私治理的利益相关者涵盖政府、企事业单位、研究人员、用户等，通过这些多元利益主体的协同治理，可获得最优治理效果。科学数据共享中的隐私治理是治理对象、治理对策与治理主体有机统一。在采取治理对策过程中，其治理效果的作用对象，不仅包含隐私相关利益主体、共享平台、共享过程，同样也包含法律保障、技术水平、数据质量等，最终以实现科学数据共享价值最大化和隐私风险最小化为治理目标。

4　科学数据共享中的隐私治理对策

根据科学数据共享中的隐私治理框架，可以从隐私法律、隐私配套制度、隐私保护技术、隐私素养、伦理、数据流程管理等 6 个方面展开推进科学数据共享中的隐私治理。

4.1　完善隐私保护法律体系

完善科学数据共享中的隐私保法律体系可从以下三方面推进：

4.1.1　推进多领域多层级隐私保护法律体系的形成

首先，应加快推进我国隐私保护的全国性系统立法，为隐私保护提供上位法支撑，并促进隐私立法在民法、行政法、刑法之间的合理衔接，互相呼应。从立法角度明确界定隐私权的概念及保护范围，对隐私权的保护作出全面、系统、层级分明的规定是弥补我国当前隐私法律体系不足的重中之重。其次，应建立健全我国多领域隐私保护法律体系，填补和完善现有隐私法律保护条款规则。如加快推进隐私权保护的专项立法进程，加快《个人信息保护法》《数据安全法》等领域单独立法的进程，提升隐私法律保护的系统性和针对性。再次，虽目前将科学数据共享中的隐私法律建设上升到颁布专门法的层面还不现实，但可针对科学数据共享中的隐私制定直接保护的原则或条款，细化具体实施行政法规细则或颁布规范性文件。

4.1.2　加强侵权责任法律保护与救济力度

在科学数据共享中的隐私侵权法律保护可引入惩罚赔偿制度，明确侵权归责原则，落实隐私侵权责任主体，加大对隐私侵权行为的处罚问责与救济力度。传统的隐私侵权可能采取停止侵权、名誉恢复、赔礼道歉等赔偿措施，但在科学数据共享环境中，这种追责方式难以对侵权行为起到较好的慑止作用。可对隐私侵权行为要求精神损害和财产损害赔偿，针对科学数据共享中的隐私侵权责任人获利所得要求赔偿。尤其对涉及范围较广、无法明确受害主体的隐私侵权事件，应加大行政处罚与经济处罚力度，减少社会影响，如 Facebook 因大规模数据泄露而被判 50 亿美元巨额罚款并整改[66]。此外，还应完善隐私侵权救济司法途径，明确救济方式和救济范围，对于行政隐私侵权事件可采取行政诉讼或民事诉讼程序协调，通过司法程序和司法解释弥补现有法律的不足。

4.1.3　加强隐私法律保护模式的国际借鉴和合作

我国科学数据共享中的隐私保护还与发达国家地区存在一定差距，可借鉴学习其他国家成熟的隐私法律保护方式，如欧盟颁布的《一般数据保护条例》。在跨境科学数据的隐私治理上，以尊重本国或本地区基本的民族权利为前提，加强国际监管与合作。

4.2　加强隐私保护配套制度建设

科学数据共享中的隐私治理制度建设，除加快隐私保护法律制度建设外，还需配套制度补充达到更好的治理效果，建议采取以下对策：

4.2.1　建立科学数据共享中的隐私保护监管制度

在科学数据共享过程中，应对涉及隐私风险的数据与行为都加以严格监管，明确监管范围，制定合理的监管和审查制度。其次，还可以发动社会监管渠道，成立第三方监管平台，公正使用监督权利并反馈监督意见。或者成立专门的科学数据隐私监管部门和数据保护官，负责监控、处理隐私侵权事件。

4.2.2　建立隐私风险评估机制

构建科学数据共享中的隐私数据风险评估体系，

有利于挖掘和发现潜在隐私风险,主动规避、控制科学数据共享中的隐私泄露与隐私侵权问题,加强隐私保护;也有利于促进公众了解科学数据共享中的隐私侵权行为和提升隐私保护能力,培育科学数据共享环境中隐私保护的氛围。

4.2.3 建立行业自律机制

科学数据共享中的法人机构,如组织者、发布者、传播者、利用者等应建立适合环境和自身特点的隐私保护自律机制和行业规范,加强责任意识,推进行业标准的细化,重视用户的权益,为用户创造信任的环境。这些法人机构应该让科学数据共享过程更加透明化,针对过程中涉及隐私的内容有义务让用户"知情同意",在告知使用目的取得同意后再开发使用。如可建立隐私保障信息共享平台,畅通隐私管理沟通渠道,让用户及时维护自身隐私权益。其次,应鼓励倡导积极开发隐私保护技术,形成良好的行业技术环境,引导规避"算法歧视",让技术引发的隐私风险通过技术更新解决,并制定隐私安全技术考核标准,定期检查隐私风险。还可以成立科学数据隐私泄露安全举报中心,形成良好的行业自律规则。

4.3 采用隐私增强技术

技术是科学数据共享中的一把双刃剑,一方面技术发展推动科学数据流动更加自由、共享、透明,另一方面也让科学数据处在"第三只眼"监控状态下,隐私保护问题日益突出。相对于隐私法律保护受限于地理区域或行业领域,隐私保护技术的应用可减少因行业壁垒或地域差异带来的"不平等",重视采用隐私增强技术(privacy enhancing technologies),可以让隐私保护防范于未然,隐私泄露风险关口前移,依靠技术保护,隐私主体实现自我控制和自我保护。目前隐私增强技术是依据技术予以隐私被保护的对象进行分类的,可以分为数据受访者隐私保护技术、数据所有者(管理者)隐私保护技术、用户隐私保护技术等几种不同的隐私保护技术[67]。

(1)数据受访者因为在科学数据生命周期内处于被动状态,不能在系统内保护自身的隐私数据,可以运用基于数据挖掘的隐私保护技术、基于语义的隐私保护技术等隐私增强技术来保护数据受访者的隐私。如可通过分析车辆的语义行为对车辆轨迹进行数据挖掘,从而对车辆停留敏感点的隐私进行保护,加强对车辆轨迹数据隐私的保护强度[68]。

(2)数据所有者(管理者)在隐私保护中起着核心作用,既有责任和义务保护数据受访者与用户的隐私,还要保障自身隐私不被泄露。数据所有者(管理者)可采用加密技术,因为目前最重要的隐私增强技术就是加密技术,可加密受访者的数据、用户的数据、自己的网络和数据[69]。目前加密技术还需不断更新完善,可采取同态加密的深度学习隐私保护技术[70],通过机器学习和深度学习对收集的科学数据进行加密分析计算,让用户存储在客户端的科学数据不被解密,同时企业为挖掘数据价值在密文上计算分析时也不会被解密,经服务器处理的密文返回给用户,只有用户才能解密,可有效地从"源头"解决用户隐私安全问题。也可加入新兴技术系统——区块链技术,该技术支持溯源问责的数据共享,对隐私流向进行记录,且数据存储不可更改,可以让数据管理者增强自律意识,维护数据受访者自主控制权,为隐私救济和惩治提供技术支撑[71]。

(3)用户可以在经常使用的网络搜索引擎和个性化推荐信息系统中使用隐私增强技术,如可使用网页浏览器加密插件对邮件进行加密,或使用匿名工具浏览网页,还可将浏览器设置成自动删除浏览痕迹,减少被监控和隐私泄露风险[69]320。因此,在科学数据共享过程中,隐私增强技术策略应及时调整与更新,综合运用多项隐私保护技术时注意优化配置,发挥不同技术保护模式的优势。同时更要重视隐私保护技术的研究与开发,我国隐私保护技术原创应用较少,可以借鉴学习其他国家技术,不断改进完善和创新。

4.4 提升利益相关者隐私素养

隐私素养是公众对隐私保护的陈述性知识与程序性知识的结合,主要侧重于数据共享的责任和风险[72]。在科学数据共享中,首先应提升科学数据组织者或管理者的隐私识别与隐私保护能力。因隐私治理策略与隐私利益相关者直接相关,识别这些隐私相关利益主体对处理隐私问题采取何种决策至关重要[73]。如在共享过程中采取何种访问控制策略、制定何种隐私数据保护规则等,以及这些具体策略和规则又遵从于哪些利益主体,都会受隐私相关利益主体所影响。而科学数据组织者或管理者有责任义务识别隐私相关利益主体,并高度重视、监督共享过程中涉及隐私的行为,以确保对共享过程中可能出现的隐私问题做出快速及时响应。科学数据组织者或管理者还应确保内部员工遵循隐私保护相关制度,并启动科学数据隐私教育培训,普通员工至少应该了解处理隐私数据的基本要求,但技术人员或数据保护官则应接受专业隐私保护培训[74]。

其次，应提升用户的隐私素养。用户需重新定义隐私，改变对隐私的看法，认识到隐私保护的价值和意义。尤其是科学数据相比于繁乱复杂的大数据，本身具有更精准集成的使用与开发价值，用户更应注意和重视科学数据共享过程中涉及的隐私权益与隐私保护。科学数据共享中的隐私保护不仅具有个人价值，还具有社会价值，应倡导隐私保护成为一种公共价值观，社会为大众提供一定的隐私空间，允许科学共享中合理的隐私期待，而用户在注意保护个人隐私权的同时，也应充分尊重他人隐私权，深化用户在隐私治理中的作用，这样才能塑造良好的隐私素养成长环境。提升用户隐私素养的另一途径是通过隐私素养教育，包括学习掌握相关隐私保护技术、法律保护知识、了解相关政策等来提升隐私保护与维权能力[75]。通过隐私素养教育，提高用户隐私素养知识与技能，才能缓解“隐私悖论”——用户对待隐私问题的行为与态度不统一的矛盾，如用户可通过掌握加密技术增强隐私数据保护，从而有效屏蔽科学数据共享中的监控和隐私泄露风险；还可通过运用隐私法律武器，追究科学共享过程中的隐私侵权行为与侵权责任。

4.5 构建隐私伦理保护规制

隐私治理中的技术、法律和制度约束具有一定限制性，构建隐私伦理规制能以道德手段为辅，对科学数据共享中的隐私侵权行为进行约束，可采取以下方式：一是构建通用的隐私伦理道德观。社会公共文化体系应构建通用的隐私道德准则，积极引导建立隐私保护道德共识，通过宣传培育科学数据生成者、发布者、传播者等的数据权属意识、隐私意识、平等意识和消除数据歧视，约束并规范科学数据中的共享行为，形成良好的科学数据共享生态环境。二是寻找隐私伦理决策均衡点[76]。在科学数据共享中，可通过寻找各方主体利益均衡的伦理决策点，在隐私问题上达成初步共识，均衡不同利益主体需求，减少隐私矛盾冲突，构建开放、自由、共享的伦理治理文化氛围。三是允许和重视隐私保护作为一种可工具化的协议嵌入算法计算中[77]，在机器学习不断向深度学习的发展趋势下，一方面通过隐私条款维护隐私主体权益，另一方面可破除因过度的伦理教条而限制科学数据共享的发展。

4.6 加强科学数据流程管理

加强科学数据共享中的隐私治理，除宏观上采取以上措施外，还应从微观上加强数据本身的治理，即需加强数据的流程管理。这不仅关系到科学数据共享价值的实现，也是隐私安全的重要保障基础。加强数据流程管理首先要确保数据的完整性、准确性、一致性、共享性、可用性、安全隐私性等质量要素[78]，这也与科学数据共享中的隐私治理原则相辅相成。可设置数据治理委员会，由委员会负责确保共享科学数据的质量，制定相关数据发布标准和政策，并监督企业在共享过程中遵守相关法规和标准操作程序，实现隐私保护的有效性和时效性。其次，根据科学数据生命周期特征对科学数据进行流程管控：①收集组织阶段：企业应根据需求收集科学数据，了解收集的数据类型、存储位置和方式、明确数据收集的使用目的，是否与其他组织共享以及在处理之前保存了多长时间；在组织存储科学数据过程中，合理划分科学数据类型，进行隐私风险分析，区分隐私数据的保护等级；此外，还需优化科学数据结构，定期清洗科学数据，规定存留周期，加强实时处理科学数据的效率，减少删除重复性、不完整性数据，合理处置无价值数据，确保科学数据的有效性和安全性。②发布传播和利用阶段：制定、完善科学数据隐私政策，其政策应包括企业背景陈述、基本的科学数据隐私规则，以及明确企业内数据保护的角色和责任；规范科学数据传播利用流程，并以技术手段为支撑，对科学数据全流程中的合规、合法性和风险性进行监控并不断改进升级，在增强科学数据的利用效果、价值基础上加强对隐私数据的防护与安全控制。

5 结语

综上可知，科学数据共享中的隐私治理是推进科学数据共享进程中不可避开的议题，是加强科学数据治理能力的必然要求。为更好地实现“科学数据共享价值的最大化”与“隐私风险的最小化”治理目的，科学数据共享中的隐私治理需政府、企事业单位、研究人员和用户等多主体积极参与、协同治理。本文基于我国科学数据共享中的隐私问题进行调研分析，提出基于数据权属与公私权利、收集限制与目的明确、公开性与安全性、多主体治理4个方面的隐私治理原则并构建了隐私治理模型，探索了适合我国科学数据共享中的隐私治理对策，提出了从法律、配套制度、技术、隐私素养、伦理、数据流程等6个维度推进科学数据共享中的隐私治理。本研究还存在一些不足之处，研究停留在对科学数据共享中的隐私治理的理论探索阶段，针对治理对策实施的治理成效检验，则有待后续进一步深入研究。

参考文献：

[1] BURKE B. Information protection and control survey: data loss pre-

vention and encryption trends[EB/OL]. [2020-07-20]. https://www.idc.com/downloads/IPC_Special_Report_One_Pager_v1.pdf.
[2] STOLL M. A data privacy governance model the integration of the General Data Protection Regulation into standard based management systems[J]. International journal of IT/business alignment and governance, 2019, 10(1): 74-93.
[3] 王利明. 人权法新论[M]. 长春:吉林出版社, 1994: 482.
[4] Data privacy: safeguarding trusted data[EB/OL]. [2020-07-20]. https://www.talend.com/resources/data-privacy/.
[5] BELYH A. Data privacy[EB/OL]. [2020-07-20]. https://www.cleverism.com/lexicon/data-privacy/.
[6] BELANGER F, CROSSLER R E. Privacy in the digital age: a review of information privacy research in information systems[J]. Mis quarterly, 2011, 35(4): 1017-1042.
[7] 张玥,朱庆华. 国外信息隐私研究述评[J]. 图书情报工作, 2014, 58(13): 140-148.
[8] GURSOY M E, LIU L, TRUEX S, et al. Differentially private and utility preserving publication of trajectory data[J]. IEEE transactions on mobile computing, 2019, 18(10): 2315-2329.
[9] 耿希,顾翠峰,马俊坚. 欧盟《一般数据保护条例》对我国患者隐私保护的启示[J]. 中国医学伦理学, 2019, 32(8): 1000-1003, 1009.
[10] 弓永钦. 欧盟数据隐私新规则对我国"涉欧"数字企业的影响及应对[J]. 国际经济合作, 2019(2): 70-79.
[11] VON BOMHARD N, AHLBORN B, MASON C, et al. The trusted server: a secure computational environment for privacy compliant evaluations on plain personal data[J]. Plos one, 2018, 13(9): 1-19.
[12] JONES E M, SHEEHAN N A, MASCA N, et al. Data shield - shared individual-level analysis without sharing the data: a biostatistical perspective[J]. Norsk epidemiologi, 2012, 21(2): 231-239.
[13] 黄国彬,刘馨然,张莎莎. 英澳科学数据共享过程中个人隐私保护政策研究[J]. 图书情报知识, 2017(6): 105-113.
[14] 冯登国,张敏,叶宇桐. 基于差分隐私模型的位置轨迹发布技术研究[J]. 电子与信息学报, 2020, 42(1): 74-88.
[15] DOVE E S. The EU general data protection regulation: implications for international scientific research in the digital era[J]. The journal of law, medicine & ethics, 2019, 46(4): 1013-1030.
[16] 史婷瑶,马金刚,曹慧,等. 医疗大数据隐私保护技术的研究进展[J]. 中国医疗设备, 2019, 34(5): 163-166.
[17] 施炎峰. 面向云平台隐私数据保护的加密技术研究[D]. 北京:北京交通大学, 2015.
[18] WALLACE S E, GAYE A, SHOUSH O, et al. Protecting personal data in epidemiological research: data shield and UK law[J]. Public health genomics, 2014, 17(3): 149-157.
[19] 李善青,郑彦宁,邢晓昭,等. 科学数据共享的安全管理问题研究[J]. 中国科技资源导刊, 2019, 51(3): 11-17.
[20] DITTERT N. Tropical research and scientific data management-why one doesn't work without the other: international conference on marine data and information systems[C]//Istituto Nazionale di Oceanografia e di Geofisica Sperimentale-OGS. International conference on marine data and information systems. Barcelona: Bollettino di Geofisica Teorica ed Applicata, 2018:303-304.
[21] YOGARAJAN V, MAYO M, PFAHRINGER B. Privacy protection for health information research in New Zealand district health boards[J]. New Zealand medical journal, 2018, 131(1485): 19-26.
[22] MACKENZIE I S U, MANTAY B J, MCDONNELL P G, et al. Managing security and privacy concerns over data storage in healthcare research[J]. Pharmacoepidemiology and drug safety, 2011, 8(20): 885-893.
[23] 温亮明,张丽丽,黎建辉. 大数据时代科学数据共享伦理问题研究[J]. 情报资料工作, 2019, 40(2): 38-44.
[24] 叶冠成,江雯欣,代逸丹,等. "开放科学"发展中的伦理问题探究——基于医学开放科学领域的分析[J]. 医学与哲学, 2019, 40(15): 32-36.
[25] DENNEDY M F, FOX J, FINNERAN T R. The privacy engineer's manifesto: getting from policy to code to QA to value [M]. New York: Apress, 2014: 42-56.
[26] DONEDA D, ALMEIDA V A F. Privacy governance in cyberspace [J]. IEEE Internet computing, 2015, 19(3): 50-53.
[27] 毕达天,曹冉,杜小民. 科学数据共享研究现状与展望[J]. 图书情报工作, 2019, 63(24): 69- 77.
[28] 黄如花,刘龙. 我国政府数据开放中的个人隐私保护问题与对策[J]. 图书馆, 2017,(10): 1-5.
[29] 王春晖,程乐. 解读民法典"隐私权和个人信息保护"[J]. 南京邮电大学学报(社会科学版), 2020, 22(3): 1-14.
[30] 邢文明,洪芳林,李晓妍. 科学数据管理体系的二维视角——《科学数据管理办法》解读[J]. 图书情报工作, 2019, 63(23): 30-37.
[31] 韩家铭. 欧盟及英国个人数据保护法的最新发展及对中国立法的启示[D]. 北京:北京外国语大学, 2019.
[32] 孙泽龄. 大数据背景下域外隐私保护法现状及对我国的启示[J]. 中国管理信息化, 2019, 22(10): 209-210.
[33] 关健. 医学科学数据共享与使用的伦理要求和管理规范(二)隐私变迁与挑战[J]. 中国医学伦理学, 2020, 33(3): 288-293.
[34] 陈刚. 开放政府数据下个人隐私的法律保护问题研究[D]. 南京:南京大学, 2017.
[35] 金元浦. 论大数据时代个人隐私数据的泄露与保护[J]. 同济大学学报(社会科学版), 2020, 31(3): 18-29.
[36] 罗芊怡. 论个人数据权跨境侵权纠纷的法律适用问题[D]. 北京:外交学院,2020.
[37] 陈仕伟,黄欣荣. 大数据时代隐私保护的伦理治理[J]. 学术界, 2016,(1): 85-95.
[38] 工业和信息化部信息通信管理局. 关于侵害用户权益行为的APP通报(2020 年第二批)[EB/OL]. [2020-07-20]. ht-

tp://www.gov.cn/xinwen/2020-07/05/content_5524298.htm.
[39] 新华社.国家计算机病毒应急处理中心监测发现 20 余款违规移动应用[EB/OL].[2020 - 07 - 20]. http://www.gov.cn/xinwen/2020-04/10/content_5500961.htm.
[40] 孙卓,孙福强.基于制度信任构建用户大数据隐私制度保护体系[J].图书馆学研究, 2018(17): 98 - 101.
[41] 王韫.大数据时代隐私权的保护[D].济南:山东大学, 2019.
[42] 谷勇浩,郭振洋,刘威歆.匿名化隐私保护技术性能评估方法研究[J].信息安全研究, 2019, 5(4): 293 - 297.
[43] CSDN 确认:600 万用户账号密码泄漏[EB/OL].[2020 - 07 - 20]. http://roll.sohu.com/20111223/n330005361.shtml.
[44] 王平水,王建东.匿名化隐私保护技术研究综述[J].小型微型计算机系统, 2011, 32(2): 248 - 252.
[45] VAN PANHUIS W G, PAUL P, EMERSON C, et al. A systematic review of barriers to data sharing in public healthy[EB/OL].[2020 - 07 - 20]. https://bmcpublichealth.biomedcentral.com/articles/10.1186/1471-2458-14-1144.
[46] 彭桥,肖尧,陈浩. APP 用户数据交易与隐私保护问题研究——对比讨价还价与甄别定价两种交易模式[J].产经评论,2020,11(3):5 - 15.
[47] 顾理平,杨苗.个人隐私数据“二次使用”中的边界[J].新闻与传播研究,2016,23(9):75 - 86,128.
[48] 360 互联网安全中心. 2017 政企机构信息泄露形势分析报告[EB/OL].[2020 - 07 - 20]. http://zt.360.cn/1101061855.php? dtid = 1101062514&did = 490913483.
[49] 张捷.当前公众的信息安全意识与隐私观念调查报告[J].国家治理,2020,(14):44 - 48.
[50] 易斌,郭华,刘颖,等.我国读者隐私权的行业自律保护研究[J].情报理论与实践,2015,38(1): 67 - 70.
[51] 信息安全与通信保密杂志社.盘点 2020 上半年全球重大数据泄露事件[EB/OL].[2020 - 07 - 20]. http://www.iscсc.gov.cn/xwdt/xwkx/07/903972.shtml.
[52] 王飏濛.边界与圈子 - 隐私悖论的形成机制[D].南京:南京师范大学, 2019.
[53] 赵芳霞.社交媒体用户隐私泄露、侵犯与保护研究[D].兰州:兰州财经大学, 2019.
[54] 中国银保监会消费者权益保护局.中国银保监会消费者权益保护局关于中信银行侵害消费者合法权益的通报[EB/OL].[2020 - 07 - 20]. http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html? docId = 903298&itemId = 925.
[55] 陈朝兵,郝文强.国内外政府数据开放中的个人隐私保护研究述评[J].图书情报工作, 2020, 64(8): 141 - 150.
[56] 艾琼,刘纯璐,游林.科研用户访问国外学术数据库的隐私保护与对策[J].图书情报工作, 2019, 63(10): 12 - 20.
[57] 汪怀君,汝绪华.人工智能算法歧视及其治理[J].科学技术哲学研究, 2020, 37(2): 101 - 106.
[58] 刘俊东.人类基因数据共享伦理研究[D].长沙:湖南师范大学, 2018.
[59] 关健.医学科学数据共享与使用的伦理要求和管理规范(一)前言[J].中国医学伦理学, 2020, 33(2): 143 - 146.
[60] 杨子飞.隐私的终结?——论大数据监控时代传统隐私伦理基础的瓦解[J].武汉科技大学学报(社会科学版), 2020, 21(4): 424 - 428.
[61] 丁晓东.数据到底属于谁?——从网络爬虫看平台数据权属与数据保护[J].华东政法大学学报, 2019, 22(5): 69 - 83.
[62] 王如.档案法律关系下公权力与私权利关系研究[D].合肥:安徽大学, 2018.
[63] 刘新宇.大数据时代数据权属分析及其体系构建[J].上海大学学报(社会科学版), 2019, 36(6): 13 - 25.
[64] 李亚娟.数字化疫情防控如何保护个人信息[N].学习时报, 2020 - 03 - 06(3).
[65] 李平原.浅析奥斯特罗姆多中心治理理论的适用性及其局限性——基于政府、市场与社会多元共治的视角[J].学习论坛, 2014, 30(5): 50 - 53.
[66] 孟雨. 2019 年多达一千多万条数据遭泄露[J].计算机与网络, 2019,45(24):14.
[67] NAVARRO-ARRIBAS G, TORRA V. Advanced research in data privacy[M]. Cham: Springer International Publishing, 2015: 6 - 7.
[68] 陶健.基于语义的隐私保护车辆轨迹数据挖掘技术研究[D].芜湖:安徽师范大学, 2018.
[69] 施耐尔.数据与监控信息安全的隐形之战[M].李先奇,黎秋玲,译.北京:金城出版社, 2018: 319 - 322.
[70] 唐鹏,黄征,邱卫东. 深度学习中的隐私保护技术综述[J].信息安全与通信保密, 2019(6): 55 - 62.
[71] 孟小峰,刘立新.区块链与数据治理[J].中国科学基金, 2020, 34(1): 12 - 17.
[72] 邓胜利,王子叶.国外在线隐私素养研究综述[J].数字图书馆论坛, 2018(9): 66 - 72.
[73] BHANSALI N. Data governance creating value from information assets[M]. New York: CRC Press, 2014: 125 - 129.
[74] How to implement a data privacy strategy-10 steps[EB/OL].[2020 - 07 - 20]. https://resources.infosecinstitute.com/how-to-implement-a-data-privacy-strategy-10-steps/.
[75] PARK Y J. Digital literacy and privacy behavior online[J]. Communication research, 2013, 40(2): 215 - 236.
[76] 薛孚,陈红兵.大数据隐私伦理问题探究[J]. 自然辩证法研究, 2015, 31(2): 44 - 48.
[77] 田海平,刘程.大数据时代隐私伦理的论域拓展及基本问题——以大数据健康革命为例进行的探究[J].伦理学研究, 2018(3): 67 - 72.
[78] 韩俊红.数据治理视角下教育数据质量模型的构建[D].北京:北京邮电大学, 2019.

作者贡献说明:

朱贝:论文写作;

王传清:框架设计与论文修订。

朱贝，王传清. 我国科学数据共享中的隐私治理探析[J]. 图书情报工作,2020,64(22):37－47.

Analysis on Privacy Governance in Scientific Data Sharing in China

Zhu Bei[1] Wang Chuanqing[2]
[1] Guangzhou Medical University Library, Guangzhou 511436
[2] National Science Library, Chinese Academy of Science, Beijing 100190

Abstract: [**Purpose/significance**] Aiming at the privacy problems in the current scientific data sharing of China, this paper explored the privacy governance methods and countermeasures in order to realize the scientific data sharing better. [**Method/process**] On the basis of clarifying the privacy problems in scientific data sharing, this paper proposed four principles of privacy governance, constructed a privacy governance model, and explored countermeasures for privacy governance in scientific data sharing by using the methods of literature survey and modelling. [**Result/conclusion**] Privacy governance can be implemented by improving the legal system of privacy protection, strengthening the construction of supporting system of privacy protection, adopting privacy enhancement technologies, improving the privacy literacy of stakeholders, establishing rules of privacy ethics protection, and strengthening the process management of scientific data to effectively promote scientific data sharing.

Keywords: scientific data sharing privacy governance governance countermeasures

《图书情报工作》2020 年选题指南

[**编者按**]本选题指南是根据本刊的定位、性质与发展需要，结合图情档学科前沿热点及当前与未来需要解决的重要问题，邀请本刊编委和青年编委为本刊策划定制，再经编辑部整理、修改和补充而形成的。这是本刊 2020 年度关注、报道的重点领域(包括但不限于这些选题)，供作者选题和研究以及向本刊投稿时的参考和借鉴。

1. 中国特色图情档学科体系、学术体系、话语体系建设
2. 图情档一级学科建设与融合发展战略
3. 图书馆“十四五”规划编制的关键问题
4. 国家文献信息资源保障能力及其建设
5. 开放科学背景下信息资源建设问题
6. 全民阅读中图书馆的定位与担当
7. 图书馆空间服务的理论与实践
8. 嵌入式学科服务的绩效评价与管理
9. 公众科学、科学素养与泛信息素养
10. 图书馆服务本科教育的模式与能力
11. 图书馆文化传承与文化育人的理论与实践
12. 图书馆出版与出版服务
13. 新媒体时代图书馆科学传播的功能与实践
14. 图书馆营销推广的战略与策略研究
15. 图书馆泛合作研究的实践与理论
16. 国家区域发展战略下图书馆联盟建设与创新服务
17. 网络空间治理的情报学问题
18. 知识产权信息服务能力与效果评估
19. 信息分析中的新技术与新方法
20. 情报服务标准化与评价
21. 数字人文与数字学术的研究与实践
22. 人工智能在图情档中的应用
23. 图书馆智能服务与智慧服务
24. 开放数据生态中的元数据发展模式研究
25. 开放科学数据行为及其模型构建
26. 数据资源建设与数据馆员能力建设
27. 大数据时代信息组织与知识组织
28. 科学数据管理与服务
29. 学术成果监测与学科竞争力分析
30. 情报计算(计算情报)的理论与方法
31. 情报分析服务质量与效能评价
32. 情报研究与智库研究的关系
33. 科学与技术前沿分析理论与方法
34. 健康中国 2030 战略下的健康信息学
35. 人机交互行为及服务模式创新
36. 图情档在新型智库建设中的作用机制
37. 智能信息服务的理论和方法
38. 数字公共文化资源、服务与体系建设
39. 数据时代政务信息资源管理和开发利用
40. 数字档案馆生态系统治理策略
41. 档案数据治理理论与治理体系
42. 政府数据开放平台应用与评价
43. 社会记忆视角下档案信息资源整理、保护与开发
44. 民族文献遗产产业化开发与利用
45. 图情档学科教育模式与人才培养能力